VIA PadLock Hardware Security Suite

Providing the Hardware Building Blocks for Optimizing Information Security

Cool Processing!

VIA Technologies, Inc.
May 2004

VIA we connect

Table of Contents

Introduction

With the VIA PadLock Hardware Security Suite, VIA has taken a unique approach to enabling advanced levels of security and privacy protection in PCs and the emerging new generation of smart connected digital devices by integrating advanced security features such as a dual random number generator and an AES encryption engine into the hardware of its growing range of VIA Eden™, VIA C3™, and VIA Antaur™ processors.

This hardware-based approach is not only inherently more secure than software-based alternatives promoted by other vendors, but it is also much more efficient in terms of overall system performance. By performing most of the heavy calculations associated with security programs in hardware, the VIA PadLock Hardware Security Suite enables high performance in demanding security applications without stressing system resources and affecting normal operation. This enables the development of small form factor, power efficient x86 consumer electronics and embedded devices that can be used for online entertainment associated with e-commerce and digital rights management.

With the forthcoming launch of the C5J Esther core, VIA is further extending the feature set of the VIA PadLock Hardware Security Suite to include support for execution (NX) protection, Montgomery Multiplier support for expediting RSA encryption, and a Secure Hash (SHA-1 and SHA-256) algorithm.

This document provides an introduction to these new features, as well as an overview of the other components contained in the VIA PadLock Hardware Security Suite.

Approaches to Security

Software-Based Security

Recognizing the need for greater security, the PC industry has been working towards improving security applications through creating standard procedures for protection of digital content; however, these procedures have been largely software-based and as a result are highly processor intensive.

This conventional approach to system design pushes the limits of even the most powerful CPUs, often resulting in flaws in other applications running at the same time as the security programs. In home entertainment applications, for example, this is totally unacceptable because consumers will not tolerate digital media centers that pause during a video while exchanging secret information with a web site.

The availability of excess CPU cycles for software-based security operations is often listed as one of the most important reasons for upgrading to multi-gigahertz processors. However, these processors are not always practical for the fast emerging consumer electronics and mobile smart digital device categories because they consume enormous amounts of power, generating too much heat for compact designs.

The VIA Hardware Approach

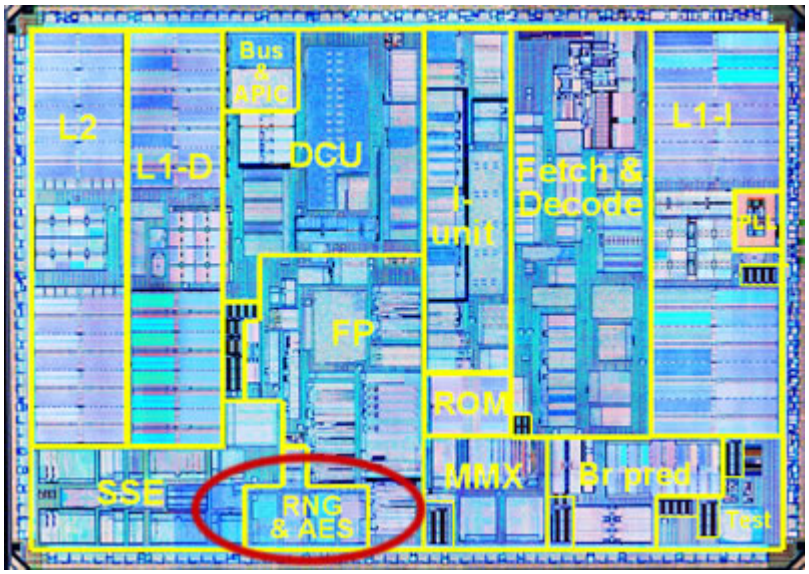
VIA has adopted a more holistic platform approach to information security through the VIA PadLock Security Initiative, systematically integrating a growing number of critical security features directly onto the processor die. These hardware-based security building blocks comprise the VIA PadLock Hardware Security Suite.

This approach manages the workload when the system is running security related applications by allocating specific operations to various VIA PadLock components, helping to achieve significantly improved performance of those operations with lower system overheads.

The VIA PadLock Hardware Security Suite

The VIA PadLock Hardware Security Suite as featured on current C5P Nehemiah core processors, consists of the VIA PadLock Random Number Generator (RNG) and the VIA PadLock Advanced Cryptography Engine (ACE). These on-die features can be accessed through dedicated x86 instructions that make them inherently more secure than software or security features integrated into the chipset and require vulnerable software drivers for operation. The figure below shows where the VIA PadLock RNG and VIA PadLock ACE reside on the C5P Nehemiah processor core.

Figure 1: A Die-plot of the C5P Nehemiah core



The Need for Good Random Numbers

The recent explosive growth of PC networking and Internet based commerce has significantly increased the need for a wide variety of computer security mechanisms. Good random numbers are essential to the following major components of computer security:

Confidentiality: Data encryption is the primary mechanism for providing confidentiality. Many different encryption algorithms exist (symmetric, public-key, one-time pad, etc), but all share the critical characteristic that the encryption/decryption key must not be easily predictable. To ensure that keys cannot be easily guessed, random number generators are used to produce cryptographic keys and other secret parameters in virtually all serious security applications.

Authentication: Challenge/response authentication protocols require that challenge values be as unpredictable as possible to ensure that attackers cannot re-use data from previous authentication transactions. The strength of passwords

used to protect access and information also depends on the difficulty of predicting or guessing the password. As a result, strong random number generators are necessary to automatically generate strong passwords.

Integrity: Digital signatures and message digests are used to guarantee the integrity of communications over a network. Random numbers are often used in digital signature algorithms to make it difficult for a malicious party to forge the signature. Many signing algorithms, including the U.S. Government's Digital Signature Standard also require random sources to ensure the security of the signing keys.

In short, good security requires good random numbers.

The VIA PadLock RNG

To address this need for good random numbers in security applications, VIA developed the VIA Padlock RNG, integrating a high-performance hardware-based random number generator onto the processor die. This RNG uses random electrical characteristics on the processor chip to generate highly random values at an extremely fast rate. It provides these numbers directly to security applications via a new x86 instruction that has built-in multi-tasking support.

Capable of creating random numbers at rates of between 1600K to 60M bits per second (depending on the quality of randomness required), the VIA PadLock RNG addresses the needs of security applications requiring true randomness

The VIA PadLock RNG uses asynchronous multi-byte generation: the hardware generates random bits at its own pace. These accumulate into hardware buffers with no impact on program execution. Software may then read the accumulated bits at any time. This asynchronous approach allows the hardware to generate large amounts of random numbers completely overlapped with program execution. This is opposed to good software generators, which can be fast but can consume a significant number of CPU cycles, thereby affecting overall system performance.

The VIA PadLock RNG has undergone comprehensive testing by leading data security firm, Cryptography Research, Inc.; results show high-performance, high-quality entropy and ease of use. See the complete Cryptography Research report, "Evaluation of VIA C3 Random Number Generator," dated February 27, 2003. For more on the VIA PadLock RNG, visit the VIA PadLock Hardware Security Suite website.

AES Encryption

Short for Advanced Encryption Standard, AES is a highly advanced data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen.

After a rigorous multi-year evaluation process, in 2001 the US Government choose AES as the new government standard (FIPS-197) replacing the older DES encryption standard. AES provides far greater security through much larger key size and an improved encryption algorithm.

AES encrypts and decrypts 128-bit blocks of data with 3 standard key lengths.
1) 128-bit key length that corresponds to approx. 3.4×10^{38} keys
2) 192-bit key length corresponding to approx 6.2×10^{57} keys
3) 256-bit key length corresponding to approx. 1.1×10^{77} keys

By comparison, DES has approx. 7.2×10^{16} keys. To try and put this into perspective, if we assumed a super-computer could break the DES code in one second, it would take the same super computer 149 thousand billion years to decode an AES key with a 128-bit key length.

AES encryption is also particularly well suited for electronic devices such as PCs, IP and mobile phones, PDAs, firewalls, and wireless standards, such as the high-speed 802.11g standard.

The VIA PadLock Advanced Cryptography Engine (ACE)

VIA C5P Nehemiah core processors integrate a powerful Advanced Cryptography Engine (ACE) that can encrypt or decrypt data at a sustained rate of 12.8Gb/s. This is faster than any known commercial AES hardware implementation, and several times faster than software implementations carried out with the latest high performance processors.

VIA PadLock ACE directly supports all three AES key sizes (128-bits, 196-bits, and 256-bits) in hardware, and with the same performance. In addition to a single application being able to use VIA PadLock ACE, any number of tasks may use it concurrently without requiring supplemental task management by the application or the operating system. Although implementation of VIA PadLock ACE contains an additional x86 state, the tasks using it do not need to save and restore this state - the hardware manages the additional state in a transparent fashion.

Table 1 below indicates how the VIA PadLock ACE provides encryption/decryption at speeds in orders of magnitude faster than a high-speed Intel® Pentium® 4 processor with approximately only half of the CPU utilization.

Table 1: AES Encryption Performance Comparison

AES Encryption Performance comparison with the VIA PadLock ACE						
Cipher Engine	1GHz VIA C3 Processor			2.4GHz Intel® Pentium® 4 Processor		
	Encrypt (in Mbps)	Decrypt (in Mbps)	Ciphering 1 GB data (in Sec)	Encrypt (in Mbps)	Decrypt (in Mbps)	Ciphering 1 GB data (in Sec)
EBC	15073.28	133255.66	0.57	106.79	93.90	8.006
CBC	6196.13	6844.87	1.23	100.64	89.38	8.450
CFB	6315.29	6699.24	1.23	100.58	99.72	7.988
OFB	3245.59	3311.29	2.44	10.83	100.98	7.928
Avg. CPU Utilization	**54%**			**99%**		

VIA PadLock ACE has been evaluated by leading data security firm, Cryptography Research, Inc. Download the Cryptography Research Preliminary Evaluation of PadLock ACE from any VIA processor web page. The VIA Nehemiah Advanced Cryptography Engine Programmers Guide is also freely available for download.

More VIA PadLock ACE test results are available from well-known cryptography expert, Dr. Brian Gladman; please visit his website at: http://fp.gladman.plus.com/ACE/.

The "Full Monty" of Hardware Based Security Features

The newly announced VIA C5J Esther core introduces three new hardware based security features to low power x86 VIA processors, extending the VIA PadLock Hardware Security Suite to include support for execution (NX) protection, Montgomery Multiplier support for expediting RSA encryption and a Secure Hash (SHA-1 and SHA-256) algorithm.

Execution (NX) Protection

Execution (NX) protection prevents malicious code associated with worms or viruses from executing and propagating from memory. Examples of such attacks include the recent Sasser worm and earlier Blaster and Welchia worms. The VIA C5J Esther core's NX feature marks memory with an attribute that indicates that code should not be executed from that memory, helping to prevent damage or propagation of malicious code within x86 devices. Execution (NX) protection is an important new hardware-based feature that will be supported in the Microsoft® Windows® XP Service Pack 2, ensuring wide industry adoption and extending information security further into the digital lifestyle.

RSA Algorithm

The RSA algorithm is the most widely used public-key cryptography system today and is increasingly important to e-commerce transactions that require exchanging confidential information with websites or checking access privileges. The major

challenge facing public-key cryptography is that it requires large amounts of processing power, posing a critical problem for low power consumer electronics and embedded devices especially, where breaks in video streaming or online transactions due to the heavy demands on the system during cryptographic operations can ruin the user experience. The VIA C5J Esther core features a dedicated x86 instruction that performs Montgomery Multiplication, an operation that significantly speeds up the RSA operation, thus reducing the workload on the processor during e-commerce transactions.

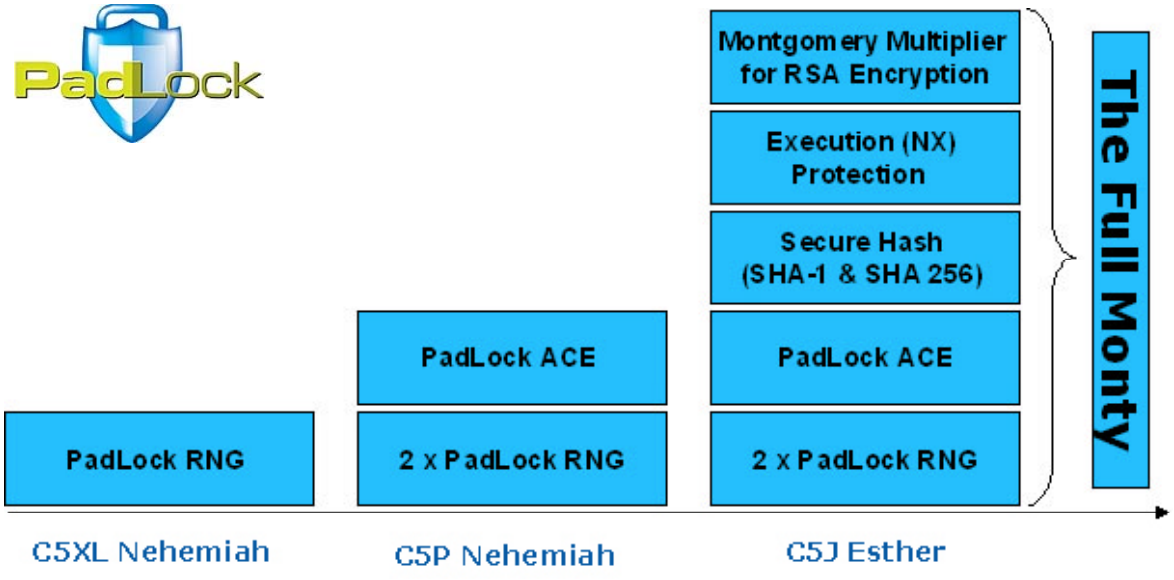
Secure Hash Algorithm

Secure Hash Algorithms are used in cryptography to provide message authentication codes (MAC) and digital signatures. These enable the recipient of information to verify the authenticity of the information's origin, and also that the information is correct. Digital signatures are increasingly being used for digital rights management and content copyright applications. The VIA C5P Esther core provides two of the most commonly used, and U.S. Government standard, Secure Hash functions (SHA-1 and SHA-256, FIPS-180-1). These assist in the creation and verification of digital signatures through algorithms that are embedded in the processor die.

VIA PadLock Hardware Security Suite: Providing the Full Monty

VIA has progressively added more hardware security features into successive processor cores and upgrades, systematically building the VIA PadLock Hardware Security Suite so that the introduction of the new C5J Esther processor core provides the "Full Monty" of security building blocks to assist communication, storage, virus protection and e-commerce security programs.

Figure 2: VIA PadLock Hardware Security Suite Roadmap



Conclusion: The Perfect Hardware Complement for Security Programs

Recognizing the need for improved security, VIA has been working for many years to develop high-performance, power efficient and affordable security features within its low power processors as part of a more holistic approach to information security. The latest C5J Esther processor core extends the VIA PadLock Hardware Security Suite into new areas of data protection, integrating various on-die building blocks designed to work in concert with secure communication, storage and e-commerce applications.

Taking on much of the heavy lifting associated with security programs, the VIA PadLock Hardware Security Suite allows high performance of demanding security applications without stressing system resources and affecting normal operation. This enables the development of small form factor, power efficient x86 consumer electronics and embedded devices that can be used for online entertainment associated with e-commerce and digital rights management.

Residing directly on the processor die, the VIA PadLock Hardware Security Suite is inherently more secure than software or chipset based security features that rely on vulnerable software drivers for operation. The VIA PadLock Hardware Security Suite consists of the VIA PadLock RNG, VIA PadLock ACE, excecution (NX) protection, secure Hash (SHA-1 and SHA-256) and support for Montgomery Multiplication that can be used for RSA encryption.

Providing the hardware building blocks for optimizing information security, the VIA PadLock Hardware Security Suite allows for better execution of demanding operations within security applications, affording greater peace of mind for consumers and business users.